FEDERAL
STUDENT AID
We Help Put America Through School

FSA Implementation Guide For Incident Reporting Procedures and Incident Handling Procedures

March 2003

Table of Contents

Draft
FSA Implementation Guide

1.0 INTRODUCTION

This document is based upon and incorporates the security incident response guidelines that the Department of Education's EDCIRC has published. The EDCIRC documents on incident response are the primary sources that should be consulted and followed. However, FSA maintains a unique and heavy dependence upon variety of contractors to run their systems. This dependence is not found elsewhere in the Department of Education. This document is written to directly address FSA's situation and concisely sets forth the roles, responsibilities and expectations FSA has for incident response.

1.1 Purpose

All Federal agencies are required by law to have within their Information Technology security programs an incident handling and reporting capability. FSA and its contracted partners operate a large number of systems at numerous locations using many different software platforms. While constructed securely, system incidents will inevitably occur. The purpose of this document is to provide guidelines and procedures for incident and potential incident handling and reporting.

1.2 Scope

FSA's Incident Response (IR) program is designed to identify, mitigate and recover from malicious and non-malicious cyber attacks. The program includes plans for notifying affected parties, escalating responses through the chain-of-command, and coordinating with the Departmental incident response team (if necessary). All FSA personnel (including contractors) are responsible for following the procedures in this document. It is especially important that Security personnel (SSO's, etc.) and those who work directly with computer systems understand and follow this document.

1.3 Definitions

FSA's Incident Response Program requires that certain terms be defined in a precise way to avoid confusion. FSA uses industry-recognized definitions, predominately based on the National Security Agency (NSA) National Security Telecommunications and Information Systems Security Committee (NSTISSI) 4009 document.

It is essential to the success of this incident response program and plan that the definitions of the supplied terms be understood and used. These terms and definitions are provided on the following page as a separate, printable sheet.

Computer Security Incident Definitions

Term		Definition
Information Assurance (NSTISSI 4009)		Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation.
IA INCIDENT TYPES	**Attack**	Involving the intentional act of attempting to bypass one or more Information Assurance Security Controls of an Information System (IS).
	Compromise	Where information is disclosed to unauthorized persons or a violation of the security policy of a system in which unauthorized internal or unintentional disclosure, modification, destruction, or loss of an object may have occurred.
	Contamination	Involving the introduction of data of one security classification or security category into data of a lower security classification or different security category.
	Denial of Service (NSTISSI 4009)	Type of incident resulting from any action or series of actions that prevents any part of an IS from functioning.
Compromised System (Based on NSTISSI 4009)		Is a system for which security measures fail to provide Information Assurance (IA).
Security Incident (Based on NSTISSI 4009)		Is an assessed occurrence resulting in a compromised system. This means that at least one the IA incident types was not stopped by currently implemented security measures.
Only when security policies and implementations fail to protect a system from these industry-recognized standards, has a security incident occurred.		

Suspicious Activity (EDCIRC)	*Any activity that is considered: an abnormal system event occurrence for a given system that cannot be immediately explained, but does not pose an immediate threat; observed recurring activity that possibly indicates attempts are being made to exploit a vulnerability but is countered by security controls in place; sporadic repeated activity that cannot be readily explained by system operations and security staff; activity that, when combined with other factors or anomalous events,* ***indicates a possible cause for concern****.* Examples of suspicious activity include: unusual usage patterns, misuse of computer system resources, or multiple attempts to log into a user account that have proven unsuccessful. (See Schedule B for more examples.)

1.4 Structure

The document is divided into four sections and an appendix. Section 1.0 has been used as an introduction and to provide definitions that affect the understanding of FSA's Incident Response Program and Plan.

Section 2.0 discusses the Incident Response Program at FSA . The roles and involvement of FSA personnel, Contractors and Department level personnel involved in implementing this program is also included in this section .

Section 3.0 provides the specifics of the Plan that FSA uses for Incident Response and Reporting. This comprises a discussion of recognizing an incident, communicating findings and the resolution of suspicious activity or security incidents. The detailed responsibilities of each of the affected parties, and how they are expected to work together, are also discussed in this section.

Section 4.0 gives a detailed and concise review of the document. It also explicitly lists the implications and impact this document places on FSA, contractors.

Finally, this document includes an appendix that gives examples of potential security incidents and other suspicious activities, how these incidents and activities might be categorized, and a form to report them that all SSOs will be expected to use.

2.0 FSA'S INCIDENT RESPONSE PROGRAM

The FSA Security IR Program is not complicated. To function properly it requires the involvement and cooperation of three groups of people: The Education Computer Incident Response Center (EDCIRC) at the Department level, FSA personnel, and FSA's numerous Contractors. Contractors are on the front lines since all FSA systems are maintained through out-sourcing contracts. Therefore, FSA's incident response program depends heavily on the Contractors. FSA personnel however, have the important role of managing and handling the security incidents and working with EDCIRC who provides the overall integration and coordination of all Incident Response services.

FSA's IR Program covers all FSA and FSA contracted systems. This includes systems on which a "risk-based decision" has been made. A risk-based decision simply indicates that the risk of a security incident of some kind to a given system is acceptable to management, but it does not remove the system from being covered and reported on under the IR Program.

2.1 EDCIRC Responsibilities

The Department of Education has established EDCIRC as the focal point and coordinator for all IR related issues throughout the Department. To provide complete IR services, contract personnel were retained and are available to provide IR capabilities for all program areas and their associated systems. EDCIRC staff will provide analysis, investigative and forensic support as necessary to those systems incapable of performing this work in-house for whatever reason. If Contractors maintaining systems are uncomfortable with this arrangement and the accompanying implications they must assume the burden of providing for these same services. EDCIRC, however will still be informed, via reporting channels described in Section 3.2 below, of all security incidents and suspicious activity for tracking and coordination purposes.

2.2 FSA Responsibilities

FSA personnel primarily maintain oversight of all contractors responsible for FSA systems. The IR policy and procedures for FSA personnel revolve around the reporting and escalation of an incident up the chain-of-command. It is not the duty of FSA staff at present to indicate the precise methods of how to accomplish IR, though it reserves the right to do so. Rather, FSA provides the contractor with the vision and mission of what is to be accomplished and lets the contractor arrange for how that vision is to be put into action. Therefore FSA allows contractors to develop their own internal IR program, though contractors must still report the incident to the appropriate FSA staff. After receiving the raw incident response and reporting information from the Contractors FSA (SSOs) then formats and files the appropriate report with EDCIRC since they are the interface for contractors to communicate with Department.

2.3 Contractor Responsibilities

The Contractor must adhere to the guidelines given in the FSA Information Technology Security and Privacy Policy (FSA Security Policy), this IR Plan, specific contract notes if applicable, Departmental policy on minimum guidelines concerning IR, and all appropriate federal laws and regulations. This indicates that the contractor is following and has documented, demonstrable industry standards in its security practices. As indicated in section 3.8 of the Security Policy, FSA must be able to show that all the appropriate preventative security tools are in place and operational. Section 4.3 of the Security Policy provides detailed information on maintaining audit logs. Because Contractors operate and maintain the systems at FSA, it falls on the individual Contractor to provide security, including the IR procedures and capabilities for the particular system or systems under their control as indicated specifically in the aforementioned sections, and to realize that such requirements are dynamic and subject to upgrade and change over time.

FSA's expectations of Contractors:

- Contractors maintaining the systems (General Support Systems or Major Applications) will provide appropriate, timely and continuous security for systems including the proper handling and recording of all incidents. If those security measures are bypassed or fail to properly protect a system the responsibility is placed on the Contractor to take any steps necessary, including adding additional tools, methods or personnel to ensure that the problem is sufficiently addressed. It is the burden of the Contractor to create and document methods and procedures to make the security controls operate effectively.

- Due to the large variety and constantly changing nature of IT platforms, devices and software being used by contractors to support FSA, FSA will not issue a listing of security settings, procedures and appropriate audit logs. It is the duty of the Contractors who maintain the systems to apprise themselves of such platform specific information or procedures as well as to implement and document them.

- FSA has imposed federal requirements to be informed of all incidents and suspicious activity whether resolved or not. Such information will be reviewed at higher levels (Department and other Federal agencies) along with information from other program areas or Agencies as the case might be, to ascertain whether there are larger trends or issues at work in the Department or Government. The Contractor must provide FSA with this information.

- At FSA it is expected that Contractors maintaining systems will have documented security incident reporting and escalation procedures. FSA recognizes that those procedures are an internal process to the Contractor. However, FSA personnel must always be an immediate part of the process when it comes to reporting, even if it requires parallel reporting.

- Contractors must provide remediation services, upgrades, patches, hot-fixes, log analysis, forensics and other security investigative and remedial services should the systems they support require it. It is also necessary for the Contractors to remain current on the upgrades, patches and hot-fixes that may apply to the systems they support. If FSA has some specific requirements that must be met in this regard FSA will make it known to the Contractor.

- Contractors must respond to and correct any Security Incident according to their own methods and procedures. But they must do so in the manner and time frame discussed in this document. Contractors are also obligated to follow FSA instruction or guidelines. FSA might also request that further or immediate investigative, forensic or remedial work be initiated or even provide standards or requirements. FSA, though, is not obligated to tell the Contractor how it should be done. Typically the Contractor is to make the decisions and to fix the problem.

- It is also within the purview of FSA management or the Department to raise the importance level of any incident, rectified or not, and to require immediate escalated action, and to direct what that escalated action might be. Such recourse would be the exception and not the normal course of action.

- If a Contractor can provide complete IR coverage including analysis, investigation and forensic services then the Department (EDCIRC) will not actively direct any part of the IR for that Contractor and their FSA systems. EDCIRC in this case will only take an active role in analysis or remediation of an incident if FSA or the Contractor asks for such involvement or when the Department can show an overriding interest to do so (i.e. inadequate contractor response, insufficiently slow response, negligence or incapability). Copies of data and information (including audits and logs) must be immediately available for Department and FSA use if it is so requested.

3.0 FSA'S INCIDENT RESPONSE PLAN

The Incident Response Program described in Section 2.0 identifies the boundaries, responsibilities and reasons for Incident Response. An Incident Response Plan uses those boundaries, responsibilities and reasons to provide the specific actions and procedures.

The Incident Response Plan used by FSA follows the guidelines provided by EDCIRC. Many items represented here can also be found in those guides.

Term	Definition
Response	A reaction to some sort of stimulus.
Incident Response	For IT Security, it is the action(s) taken by a group or individual when an activity or incident occurs that the group deems affects their security.
Incident Response Plan	A Pre-defined set of actions and responsibilities that must be taken to ensure speedy and appropriate response when suspicious activity or a security incident happens.

There are three broad areas that an IR Plan should address. They are as follows: 1) recognizing issues 2) communicating the issues and 3) the process of resolution. This plan will discuss each area and provide the required actions and responsibilities of the participants.

3.1. Recognizing issues

"What are we looking for?" is the first question that is commonly asked when thinking about IR. However, even with a page of examples (See appendix A) given there is inevitably something left out. Also, each system will have a different activity levels and different toleration levels for certain types of activity which only familiarity with the system will indicate. To this end, only a general description of what to look for can be given. In one sentence, the object of IR is to detect a Security Incident or Suspicious Activity as defined on the first pages of this document.

However, "how" to recognize Suspicious Activity or an Incident is also extremely important. Many Security Incidents are noticeable and immediately recognizable such as many hacker attacks or web defacements, or even alert notices from sensors detecting wrong behavior or change to a system. In these cases there is no need to specify "how to recognize" suspicious activity or an incident because the infraction is immediately obvious. However, other Security Incidents can only be discovered if someone is looking for the Suspicious Activity. Such discovery can only be made if there is some way of monitoring or recording events and there are consistent, routine reviews taking place. Event logs and audits are a way this can be accomplished. Any log or audit record can provide clues of suspicious activity or reveal the trail of an actual Security Incident. The first step is to research and then enable all logging and auditing functions for a given platform that will most likely help identify such activity (see Section 4.3 of FSA Security Policy for more information).

Once all determined areas of systems susceptible to inappropriate use or manipulation are monitored or their activities recorded, then those logs should be reviewed by those familiar with the system for any events, or series of events that indicate a breach in security. In order to avoid confusion FSA refers to the routine inspection of logs and audits for Suspicious Activity or Security Incidents as a "log review". The terms "analysis" and "log analysis" are terms that refer to a scrutinized inspection of data, logs and audits after Activity or Incidents are identified.

Even though some reviews can be automated there must be a frequent, routine and consistent review of all monitored and/or recorded events by a person who is familiar with the system on a daily basis. The frequency of review must be documented. The reviewer should also have an understanding of what system or network behavior is suspect or anomalous. This understanding is learned by following baselines that establish typical activity levels or thresholds.

Typically, there is activity on the logs that does not follow the general rules of the system but does not necessarily make it "suspicious activity" or a "security incident". Such an assessment would be made when logs are compared to a base-lined activity log. If the noted activity is different or of a distinctly different nature, then there is probably good cause for concern and gives reason to call the event "suspicious activity". Actually identifying an issue of concern as a "security incident" entails being able to positively know and/or show that a given activity is wrong. To move an issue previously categorized, as a "suspicious activity" into the category of a "security incident" requires research and analysis (see also sections 3.2.2 and 3.3).

Each system must retain a copy of all audit logs. Section 4.3 of the FSA Security Policy states that such logs will be kept for a minimum of one year.

All of this is the process of finding a security incident or a suspicious activity. Even if a network had an immediate security problem such as a hacker attacking the network, a rapid recourse to system logs would be invaluable as they would at least provide identifying information needed to formulate an effective response.

3.2. Communicating the Issue

There are two broad IR categories that must be reported:

- Any suspicious or anomalous incident must be reported (weekly and monthly, see below)
- A Security Incident must be reported immediately.

3.2.1 Suspicious or Anomalous Activity Process – Communicating the Issue

If a suspicious activity is investigated, further investigation can only arrive at one of three answers: no cause for concern, a Security Incident, or unknown and/or inconclusive therefore subject to further monitoring. To arrive at any of the three conclusions the following 'Suspicious Activity' Action Chain must be followed.

'Suspicious or Anomalous Activity' Action Chain

The Suspicious Activity Action Chain provided below is written from the point of view of using the IR capabilities provided by EDCIRC. If a FSA Contractor is not using this service the requirements for daily reporting to the SSO still remain the same. This also means that the Contractor will report on their analysis findings and recommendations to the SSO (who will forward the information to the FSA Incident Handling Coordinator or CSO and so on) within the specified timeframe and to show that items are being resolved.

- If, during system log reviews, suspicious activity is discovered, the reviewer will report it to the Security Engineer and thus through the internal contractor channels and also to the SSO who will categorize the activity according to the attached Schedule B, the Suspicious Activity Matrix for FSA and Department use.
- Category "A" type suspicious activity (which is effectively countered by security controls in place) will be logged and tracked by the system SSO. The SSO will provide a report on this type of activity every month. Please note that a report can be submitted at any time if there is special concern over a given activity.
- Category "B" type suspicious activity (which is effectively countered by security controls in place but its continued repetition causes additional concern). The SSO will provide a report on this type of activity every week. Please note that a report can be submitted at any time if there is special concern over a given activity.
- The FSA Incident Handling Coordinator or CSO will review and then forward all Suspicious Activity reports to the Department's Incident Handling Coordinator. The Department's Incident Handling Coordinator will review the reports and within **24-48 hours** of receipt they will convey back any findings and recommended action to the submitting office.

3.2.2 Security Incident Process – Communicating the Issue

The Security Incident Action Chain provided below is written from the point of view of using the IR capabilities provided by EDCIRC. If an FSA Contractor is not using this service the requirements for reporting to the SSO still remain the same and an incident will still be reported up the chain as described. In such a scenario, since the Contractor is providing the analysis and other Incident Response services the Department Incident Handling Coordinator and the Contractor Incident Coordinator would need to work cooperatively, but would let the Contractor handle the flow of the investigation as indicated in section 2.3.1.

The proper handling of a Security Incident means immediate action, because by definition a Security Incident implies that something has or is in the process of breaching security. If a security incident, as identified by an operator, is deemed as being a serious threat or misuse of systems and data, the affected system can be immediately taken off-line in accordance with proper shutdown/offline procedures and removed from service. In fact, taking the offending system offline should be the first action that is taken. However, this also has ramifications that are dealt with and should be studied in section 3.3. Once an Incident is identified the following chain of action will be set into motion.

'Security Incident' Action Chain

- Any observed activity that may indicate a computer security incident has occurred must be reported immediately to the relevant System Security Officer (SSO) or security administrator by telephone, email or fax. The reporting party must receive "confirmation of receipt" from the relevant SSO or security administrator; and, it is the responsibility of the reporting party to note the time receipt was confirmed. *If the relevant SSO or Security Administrator is not available by telephone, email or fax, the reporting party must notify FSA's Incident Handling Coordinator or the CSO using the same process and receipt confirmation.* (See attached Suspicious Activity Report (SAR) form for identification of the information that should be reported.) SSOs, Computer Security Officers (CSOs) and other FSA staff will be trained concerning observable indicators that suggest an incident may have occurred.
- The SSO will ensure that all information on the Suspicious Activity Report (SAR) has been filled out. The SSO must then notify FSA's Incident Handling Coordinator or CSO by telephone, email or fax within **one (1) hour** of receiving the initial SAR. If neither person is available by telephone, email or fax, the reporting party must notify the OCIO Incident Handling Coordinator using the same process and receipt confirmation. *If the OCIO Incident Handling Coordinator has not confirmed receipt within one (1) hour of notification, the reporting party must notify the Deputy CIO using the same process and receipt confirmation.* FSA's Incident Coordinator or CSO reviews the initial SAR, and related information to determine whether a potential incident has occurred. That person then reports the potential incident and all related information to the Office of the Chief Information Officer (OCIO) Incident Handling Coordinator and to his or her Principal Office senior officer within **three (3) hours** of receiving the initial report. All information will be included in a report to the OCIO Incident Handling Coordinator.
- The OCIO Incident Handling Coordinator will make a determination using Department incident handling program procedures **within one (1) hour of receiving a SAR**. If warranted, the Incident Handling Coordinator may escalate the details of the report to the Deputy CIO. If the security event or suspicious activity is deemed a serious threat to any Department's IT resources or data, the OCIO Incident Handling Coordinator will activate EDCIRC procedures and escalate the information to the Deputy CIO.
- The Deputy CIO will review the SAR **within one (1) hour** of receipt and determine whether escalation to the CIO is warranted.

- The CIO or the CIO's designee will review the SAR within **one (1) hour** of receipt and determine whether escalation to the Deputy Secretary, the Office of the Inspector General, and appropriate external officials is warranted.

Incident Reporting Chain Summary

Position	**(Reports Incident To) Position**	**Response Time**
System Administrator	System Security Officer (SSO)	Immediately
System Security Officer (SSO)	FSA Incident Coordinator or CSO	1 hour
FSA Incident Coordinator or Computer Security Officer (CSO)	OCIO Incident Handling Coordinator and PO Senior Officer	3 hours
OCIO Incident Handling Coordinator	Deputy Chief Information Officer	1 hour
Deputy Chief Information Officer	Chief Information Officer	1 hour
Chief Information Officer or CIO’s Designee	Deputy Secretary, Inspector General, and others as appropriate	1 hour

3.2.3 Updates and Status Reports – Communicating the Issue

Updates or status reports about an incident will be available from the contractor three times a day or within one-half hour of a request unless otherwise agreed upon with the Incident Handling Coordinators. The three default times for the reports will be at Open of Business, Noon and Close of Business. Updates or status reports will continue to be made until the incident is resolved or until no longer needed.

Updates are the responsibility of the party performing the research, investigation or analysis. For example, if an FSA contractor cannot provide the analytical investigative or forensic IR capabilities EDCIRC, or someone like EDCIRC can provide it for them. This puts the burden of timely communication and providing status reports and feed-back upon EDCIRC - once they receive the data, logs and audits.

3.2.4 External Notification – Communicating the Issue

The reporting of computer security incidents to the Federal Computer Incident Response Center (FEDCIRC) and the National Infrastructure Protection Center (NIPC) and other appropriate external law enforcement authorities is the responsibility of ED/OCIO and/or the Office of the Inspector General. Individual Principal Offices such as FSA and their contractors will not report potential computer security incidents to external agencies. ED/OCIO and/or the Office of the Inspector General will notify FSA and/or Contractor Incident Handling Coordinators prior to issuing an external notice.

3.3 Resolving the Suspicious Activity or Security Incident

Once suspicious activity or an actual incident is recognized and reported a period of time follows that will require the quick and consistent support and cooperation from all affected parties. The first step will be to collect data and research the extent of the problem to determine if there are additional suspicious activities or security incidents. This is accomplished primarily through in-depth log and audit analysis.

After the first step there are many different scenarios and steps that might take place before the problem is resolved or fixed. If the Contractor is relying upon EDCIRC to provide the in-depth analysis, investigation and or forensic services, they must be ready to cooperate in this process and immediately provide all details and information as needed.

Suspicious Activity
In the case of a Suspicious Activity, further analysis will show one of three conclusions: no cause for concern, a Security Incident, or unknown and/or inconclusive requiring monitoring. If the suspicious activity is concluded to be a Security Incident then the process and procedures for a Security Incident found in this document will be followed. The actions to take for the two remaining conclusions are self-defining. (See Section 3.2.1 for Suspicious Activity Chain of Events)

Security Incident
At the same time the analysis for a Security Incident is taking place, FSA expects contractors to provide an alternate, secure system that clients may continue to access if there is extended investigation. This alternate system will only be activated upon agreement between FSA Incident Handling Coordinators. This is consistent with FSA's Continuity of Support Plan (COS) and the Disaster Recovery Plan (DR). Some systems with low availability ratings may not have a COS or DR that calls for alternate system processing. In such a case the contractor should make that information known and consult with FSA on how to proceed. The proposal should be submitted as a section of a Status Report. FSA and Departmental authority must approve the proposal for the alternate system before it is placed on-line.

If a security incident is deemed a serious threat or misuse of systems and data, as identified by an operator, the affected system will be taken off-line immediately in accordance with proper shutdown/offline procedures and isolated. It is essential that this be done only after notifying an FSA or Dept. of Education authority and that it be immediately reported via the SSO to FSA's Incident Handling Coordinator as part of the Security Incident Report.

As part of resolving the Security Incident and after receiving the Findings information from a completed investigation/analysis, the Contractor must consult with FSA and the Department and propose a course of action to remedy the problem and prevent its reoccurrence. FSA, Department and Contractor parties must agree upon the course of action before implementation.

3.4 Preservation of Evidence and Final Disposal

If it is determined that the incident is likely to be criminal in nature, and that system has been taken off-line with the concurrence of a government authority and the coordination of the Incident Handling Coordinator, that system will not be tampered with or brought back on line without authorization from both FSA's and the Department's Incident Handling Coordinators. This includes but is not limited to any patch, fix, update, correction or restoration of the operational functions of the affected system(s) or physical inspection, opening or replacing of parts. This action is necessary to ensure preservation of potential criminal evidence and system condition at the time an incident was discovered.

Once the Security Incident is resolved, and the agreed upon course of action is completed the Contractor will file a final status report for approval to reestablish the system or to show final disposition if it is not reestablished. The Contractor must wait until the 'ok' is given by Incident Response Coordinators before reestablishing or otherwise disposing of any system involved in a Security Incident.

4.0 IMPACT AND IMPLEMENTATION

This document provides common, industry accepted definitions of Suspicious Activity, Security Incident and other terms. These terms were provided to avoid confusion among all those involved in FSA IR.

Notice is given that all systems are included in the Incident Response program. Details of the interaction that EDCIRC, FSA and the Contractor have in the Incident Response program are outlined. Since the Contractors are the front-line position for IR, the general expectations and possible issues relating to their duties are provided.

The need for full Incident Response Capabilities is laid out clearly. It states that if a Contractor cannot provide these capabilities then the Department has contracted with a group to provide those capabilities and all parties will have to work in cooperation.

In explaining the Incident Response Plan for FSA definitions are provided as to better understand what constitutes an Incident Response Plan. The plan details the three broad categories that Incident Response deals with, namely, 1) recognizing issues 2) communicating the issues and 3) resolving the issues.

The first category, recognizing the issues, points out that FSA is looking for Suspicious Activity and Security Incidents. To accomplish this there is a need for audits and logs (see section 4.3 of the FSA Security policy) there must be a daily review of audits and logs, and they will be retained for at least one year. To help those implementing the plan the distinction is made between “log reviews” and “log analysis”.

Under the second category of Incident Response, namely, communicating the issue, the issue of proper reporting procedures and points of contact for Suspicious Activity and Security Incidents are discussed. Also included in this area is the responsibility for updating reports and for external notification.

Of special note is:

- The establishment of a single point of contact – an Incident Handling Coordinator for FSA - and someone similar for the Contractor.
- Having the SSO’s as the primary point of contact when reporting Suspicious Activity and Security Incidents.
- The submission of weekly and monthly reports for Suspicious Activity – filed by the SSO.
- Specification of a reporting chain and time limits for Suspicious Activity and Security Incidents.
- Use of a specific form (provided) for reporting Activity or Incidents.

The third part of the incident response Plan, Resolving the Issue, emphasizes the need for research and analysis of all suspicious activities and incidents as the first step towards resolving any issue. It also addresses how and when a system may be taken off-line and also that any restoration, rebuilding, remedy or alternate system can only be made when the FSA Incident Handling Coordinator agrees.

APPENDIX CONTENTS PAGE

Flow Charts

Chart 1 - Suspicious Activity – FSA Contractors providing IR Support Services

Instructions: Follow the numbers from lowest to highest to find the next expected action. There is one action per row. Some actions require the attention of other actors before you can proceed.

Contractors	FSA	Ed or EDCIRC
1) Monitor and Review systems and logs		
2) Suspicious Activity identified		
3) System left on-line		
4) Analysis of Activity 1) Allowed activity 2) Inconclusive – mark and monitor 3) Security Incident (see Chart 3)		
5) -Weekly Report - Category A activities -Monthly Report - Category B activities	**5a)** SSO reviews Report relays it to CSO, CSO to EDCIRC	**5b)** EDCIRC reviews Reports

Chart 2 - Suspicious Activity – EDCIRC providing IR Support Services

Instructions: Follow the numbers from lowest to highest to find the next expected action. There is one action per row. Some actions require the attention of other actors before you can proceed. Please note that on rows 5 and 6 actions start in the EDCIRC column.

Contractors	FSA	Ed or EDCIRC
1) Monitor and Review systems and logs		
2) Suspicious Activity identified		
3) System left on-line		
4) -Weekly Report - Category A activities -Monthly Report - Category B activities	**4a)** SSO reviews Report relays it to CSO, CSO to EDCIRC	**4b)** EDCIRC reviews Report
		5) Analysis of Activity 1) Allowed activity 2) Inconclusive – mark and monitor 3) Security Incident (see Chart 4)
6b) Take action as advised by EDCIRC.	**6a)** Receive action and feedback report from EDCIRC	**6)** Provides analysis feed back and required action to FSA and Contractor

Chart 3 - Security Incident – FSA Contractors providing IR Support Services

Instructions: Follow the numbers from lowest to highest to find the next expected action. There is one action per row. Some actions require the attention of other actors before you can proceed.

Contractors		FSA	Ed or EDCIRC
1) Monitor and Review systems and logs			
2) Security Incident identified			
3) Notify FSA **or** EDCIRC authority for authority to take system off-line		**3a)** Approve System to go off-line	**3b)** Approve System to go off-line
4) Take system off-line, isolate and freeze			
5) File Report with SSO		**5a)** SSO reviews Report relays it to CSO, CSO to EDCIRC	**5b)** EDCIRC reviews report. Notifies FEDCIRC and others as necessary.
6) Start Status Reports: OOB, Noon and COB or as requested until resolved		**6a)** Receive first Status Report	**6b)** Receive first Status Report
7) Analysis of Incident data and system, forensics/ investigate	*STATUS REPORTS*		
8) Propose alternate/backup system Wait for approval		**8a)** Receive alt. request- Approve	**8b)** Receive alt. request from FSA - Approve
9) Implement alt. system			
10) Analysis complete, submit findings Propose course of action. Wait for FSA and EDCIRC consensus.		**10a)** Receive Findings Report meet and Consult on course of action	**10b)** Receive Findings Report meet and Consult on course of action
11) Course of action followed.			
12) Security Incident resolved Request system reestablished Wait for approval.		**12a)** System re-establishment approved.	**12b)** System re-establishment approved
13) Original system "un-frozen" fixed and reestablished.			

Chart 4 - Security Incident – EDCIRC providing IR Support Services

Instructions: Follow the numbers from lowest to highest to find the next expected action. There is one action per row. Some actions require the attention of other actors before you can proceed. Please note that rows 7, 8, and 11 actions start in the EDCIRC column.

Contractors	FSA	Ed or EDCIRC	
1) Monitor and Review systems and logs			
2) Security Incident identified			
3) Notify FSA **or** EDCIRC authority for authority to take system off-line	**3a)** Approve System to go off-line	**3b)** Approve System to go off-line	
4) Take system off-line, isolate and freeze			
5) File Report with SSO	**5a)** SSO reviews Report relays it to CSO, CSO to EDCIRC	**5b)** EDCIRC reviews report – Provides feedback and "next-step" information. Notifies FEDCIRC and others as necessary.	
6) Follow instruction from EDCIRC - provide a bit-image of system to EDCIRC.	**6a)** Follow instruction from EDCIRC		
7b) Receive first Status Report	**7a)** Receive first Status Report	**7)** Start Status Reports: OOB, Noon and COB or as requested until resolved	
		STATUS REPORTS	**8)** Analysis of Incident data and system, forensics/ investigate
9) Propose alternate/backup system Wait for approval	**9a)** Receive alt. request- Approve		**9b)** Receive alt. request from FSA - Approve
10) Implement alt. system			
11b) Receive Findings Report Consult on course of action.	**11a)** Receive Findings Report Consult on course of action		**11)** Analysis complete and findings submitted. Course of action proposed.
12) Course of action followed and completed.			
13) Security Incident resolved Request system reestablishment Wait for approval.	**13a)** System re-establishment approved.		**13b)** System re-establishment approved
14) Original system "un-frozen" fixed and reestablished.			

Examples of Suspicious Activity That Require Reporting to the OCIO. These examples are to serve as guidelines with the understanding that each appropriately responsible IT Team apply judgment based on their own environments.

Schedule A

Description	System Affected	Threshold	Reporting Chain & Timeframe For Reporting
Priority system alarm or similar indication from an intrusion detection tool and you have confirmed that it is NOT a false positive	Whether the system being affected by this type of event is part of the Mission Essential Infrastructure or not, it should be considered serious and reported as an incident to the OCIO	This should be reported at the first occurrence, as soon as it is observed and verified by the responsible team	1. Observer reports to SSO -- IMMEDIATELY 2. SSO Reports to PO CSO – WITHIN ONE (1) HOUR OF BEING NOTIFIED 3. PO CSO Reports to OCIO Incident Handling Coordinator – WITHIN THREE (3) HOURS OF BEING NOTIFIED (AND AFTER SOME INTERNAL ANALYSIS) 4. OCIO Incident Handling Coordinator Reports to the Deputy OCIO and to EDCIRC – WITHIN ONE (1) HOUR OF NOTIFICATION (AND AFTER SOME INTERNAL ANALYSIS, VERIFICATION & DETERMINATION) 5. EDCIRC begins remediation – WITHIN ONE (1) HOUR OF NOTIFICATION
Suspicious entries in system or network accounting (e.g., a UNIX user obtains root access without going through the normal sequence)			
Accounting discrepancies (e.g. someone notices a 45-minute gap in the accounting log in which no entries whatsoever appear)			
Unexplained, new user accounts			
Unexplained modification or deletion of data			
Denial/disruption of service or inability of one or more users to log in to an account			
Operation of an unauthorized program or sniffer device to capture network traffic			
Unauthorized vulnerability scanning			
Unusual time of usage (many computer security incidents occur during non-working hours)			

Examples of Suspicious Activity That Require Reporting to the OCIO. These examples are to serve as guidelines with the understanding that each appropriately responsible IT Team apply judgment based on their own environments.

An indicated last time of usage of a user account that does not correspond to the actual last time of usage for that user			**6. Deputy CIO reports to the CIO – WITHIN ONE (1) HOUR (AND AFTER SOME INTERNAL ANALYSIS, VERIFICATION & DETERMINATION) or, at his/her discretion.** **7. The CIO Reports to Secretary & Inspector General's Office & Any Required External Agencies – WITHIN ONE (1) HOUR**

Schedule B

Description	Mission Essential System Affected	Threshold	Category	Reporting Chain	Reporting Timeframe
Unauthorized Port Scanning	**N**	**<1,000 Per Week**	**A**	***Logged & Tracked By System SSO & Reported to OCIO*** **OCIO Reviews & Analyzes and responds to Reporting SSO within 24-48 Hours of Receipt**	**Monthly Report – Submitted Not later than the 4th day of the month following the month in which the activity is discovered**
	Y	**<1 Per Week**	**A**		
	N	**>1,000 Per Week**	**B**	**Logged & Tracked By System SSO & Reported to OCIO** **OCIO Reviews & Analyzes and responds to Reporting SSO within 24 Hours of Receipt**	**Weekly Report – Submitted Not later than the 4th day of the week following the week in which the activity is discovered**
	Y	**>1 Per Week**	**B**		

Examples of Suspicious Activity That Require Reporting to the OCIO. These examples are to serve as guidelines with the understanding that each appropriately responsible IT Team apply judgment based on their own environments.

Description	Mission Essential System Affected	Threshold	Category	Reporting Chain	Reporting Timeframe
A virus/worm email hoax	N	<3 Per Week	A	*Logged & Tracked By System SSO & Reported to OCIO* OCIO Reviews & Analyzes and responds to Reporting SSO within 24-48 Hours of Receipt	Monthly Report – Submitted Not later than the 4th day of the month following the month in which the activity is discovered
	Y	<1 Per Week	A		
	N	>3 Per Week	B	Logged & Tracked By System SSO & Reported to OCIO OCIO Reviews & Analyzes and responds to Reporting SSO within 24 Hours of Receipt	Weekly Report – Submitted Not later than the 4th day of the week following the week in which the activity is discovered
	Y	>1 Per Week	B		
User Account That Has been compromised	N	=1Per Week	A	Logged & Tracked By System SSO & Reported to OCIO OCIO Reviews & Analyzes and responds to Reporting SSO within 24-48 Hours of Receipt	Monthly Report – Submitted Not later than the 4th day of the month following the month in which the activity is discovered
	Y	<1 Per Week	A		
	N	>1 Per Week	B	Logged & Tracked By System SSO & Reported to OCIO OCIO Reviews & Analyzes and responds to Reporting SSO within 24 Hours of Receipt	Weekly Report – Submitted Not later than the 4th day of the week following the week in which the activity is discovered
	Y	>1 Per Week	B		

Examples of Suspicious Activity That Require Reporting to the OCIO. These examples are to serve as guidelines with the understanding that each appropriately responsible IT Team apply judgment based on their own environments.

Description	Mission Essential System Affected	Threshold	Category	Reporting Chain	Reporting Timeframe
Misuse of system resources by valid users	N	<3 Per Week	A	Logged & Tracked By System SSO & Reported to OCIO OCIO Reviews & Analyzes and responds to Reporting SSO within 24-48 Hours of Receipt	Monthly Report – Submitted Not later than the 4th day of the month following the month in which the activity is discovered
	Y	<1 Per Week	A		
	N	>3 Per Week	B	Logged & Tracked By System SSO & Reported to OCIO OCIO Reviews & Analyzes and responds to Reporting SSO within 24 Hours of Receipt	Weekly Report – Submitted Not later than the 4th day of the week following the week in which the activity is discovered
	Y	>1 Per Week	B		
Multiple unsuccessful logon attempts	N	<9 Per Week	A	Logged & Tracked By System SSO & Reported to OCIO OCIO Reviews & Analyzes and responds to Reporting SSO within 24-48 Hours of Receipt	Monthly Report – Submitted Not later than the 4th day of the month following the month in which the activity is discovered
	Y	<3 Per Week	A		
	N	>9 Per Week	B	Logged & Tracked By System SSO & Reported to OCIO	Weekly Report – Submitted

Examples of Suspicious Activity That Require Reporting to the OCIO. These examples are to serve as guidelines with the understanding that each appropriately responsible IT Team apply judgment based on their own environments.

Description	Mission Essential System Affected	Threshold	Category	Reporting Chain	Reporting Timeframe
	Y	>3 Per Week	B	OCIO Reviews & Analyzes and responds to Reporting SSO within 24 Hours of Receipt	Not later than the 4th day of the week following the week in which the activity is discovered
Unexplained new files or unfamiliar file names	N	<5 Per Week	A	Logged & Tracked By System SSO & Reported to OCIO OCIO Reviews & Analyzes and responds to Reporting SSO within 24-48 Hours of Receipt	Monthly Report – Submitted Not later than the 4th day of the month following the month in which the activity is discovered
	Y	<1 Per Week	A		
	N	>5 Per Week	B	Logged & Tracked By System SSO & Reported to OCIO OCIO Reviews & Analyzes and responds to Reporting SSO within 24 Hours of Receipt	Weekly Report – Submitted Not later than the 4th day of the week following the week in which the activity is discovered
	Y	>1 Per Week	B		
Unexplained modifications to file lengths and/or dates, especially in system executable files	N	<5 Per Week	A	Logged & Tracked By System SSO & Reported to OCIO OCIO Reviews & Analyzes and responds to Reporting SSO within 24-48 Hours of Receipt	Monthly Report – Submitted Not later than the 4th day of the month following the month in which the activity is discovered
	Y	<1 Per Week	A		

Examples of Suspicious Activity That Require Reporting to the OCIO. These examples are to serve as guidelines with the understanding that each appropriately responsible IT Team apply judgment based on their own environments.

Description	Mission Essential System Affected	Threshold	Category	Reporting Chain	Reporting Timeframe
	N	>5 Per Week	B	Logged & Tracked By System SSO & Reported to OCIO OCIO Reviews & Analyzes and responds to Reporting SSO within 24 Hours of Receipt	Weekly Report – Submitted Not later than the 4th day of the week following the week in which the activity is discovered
	Y	>1 Per Week	B		
Unexplained attempts to write to system files or changes in system files	N	<5 Per Week	A	Logged & Tracked By System SSO & Reported to OCIO OCIO Reviews & Analyzes and responds to Reporting SSO within 24-48 Hours of Receipt	Monthly Report – Submitted Not later than the 4th day of the month following the month in which the activity is discovered
	Y	<1 Per Week	A		
	N	>5 Per Week	B	Logged & Tracked By System SSO & Reported to OCIO OCIO Reviews & Analyzes and responds to Reporting SSO within 24 Hours of Receipt	Weekly Report – Submitted Not later than the 4th day of the week following the week in which the activity is discovered
	Y	>1 Per Week	B		
Unusual usage patterns (e.g., programs are being compiled in the account of a user who does not know how to program)	N	<3 Per Week	A	Logged & Tracked By System SSO & Reported to OCIO OCIO Reviews & Analyzes and responds to Reporting SSO within 24-48 Hours of Receipt	Monthly Report – Submitted Not later than the 4th day of the month following the month in which the activity is discovered
	Y	< 1 Per Week	A		

Examples of Suspicious Activity That Require Reporting to the OCIO. These examples are to serve as guidelines with the understanding that each appropriately responsible IT Team apply judgment based on their own environments.

Description	Mission Essential System Affected	Threshold	Category	Reporting Chain	Reporting Timeframe
	N	>3 Per Week	B	Logged & Tracked By System SSO & Reported to OCIO OCIO Reviews & Analyzes and responds to Reporting SSO within 24 Hours of Receipt	Weekly Report – Submitted Not later than the 4th day of the week following the week in which the activity is discovered
	Y	>1 Per Week	B		
Attempts to "Social Engineer" or otherwise convince users/administrators to provide information to unauthorized parties	N	<4 Per Week	A	Logged & Tracked By System SSO & Reported to OCIO OCIO Reviews & Analyzes and responds to Reporting SSO within 24-48 Hours of Receipt	Monthly Report – Submitted Not later than the 4th day of the month following the month in which the activity is discovered
	Y	<1 Per Week	A		
	N	>4 Per Week	B	Logged & Tracked By System SSO & Reported to OCIO OCIO Reviews & Analyzes and responds to Reporting SSO within 24 Hours of Receipt	Weekly Report – Submitted Not later than the 4th day of the week following the week in which the activity is discovered
	Y	>1 Per Week	B		